UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/539,319	03/30/2000	Takeshi Saito	0039-76672RD	7919

22850 7590 12/31/2003

OBLON, SPIVAK, MCCLELLAND, MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
NORRIS, TREMAYNE M	

ART UNIT	PAPER NUMBER
2137	6

DATE MAILED: 12/31/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/539,319	SAITO ET AL.	
	Examiner	Art Unit	
	Tremayne M. Norris	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *30 March 2000*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *30 March 2000* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. §§ 119 and 120

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☒ Certified copies of the priority documents have been received in Application No. 11/093,916.

3.☒ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

13)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

a) ☐ The translation of the foreign language provisional application has been received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *3,5*.
4) ☐ Interview Summary (PTO-413) Paper No(s). _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Claims 1-3,5-13,15-20 rejected under 35 U.S.C. 102(e) as being anticipated by Komuro et al.

Regarding Claim 1, Komuro et al teach a content information distribution apparatus for distributing encrypted content information, via a network in accordance with a prescribed transport protocol, to other end apparatus in a communication authenticated by an authentication process including at least one procedure of an authentication procedure and a key exchange procedure, comprising:

(a) a unit for encrypting content information encoded by a prescribed encoding system (col.7 lines 50-53);

(b) a unit for generating an encryption attribute header including attribute information. with regard to the encryption of the content information (col.7 lines 53-65);

(c) a unit for performing transport protocol processing required to transfer the content information and for generating a basic transport header to be added to the content information to which the encryption attribute header has been added (col.7 lines 53-65); and

(d) a unit for sending to the other end apparatus (col.7 lines 56-58) that is authenticated a packet including the basic transport header, the encryption attribute header, and the encrypted content information, wherein the encryption attribute header is set into an expansion transport header within a packet header of the packet or into a payload header within a payload to be encrypted of the packet (Figs 4, 5A, 5B; col.7 line 30 thru col.10 line 58) .

Regarding Claim 2, Komuro et al teach the apparatus according to claim 1, wherein the encryption attribute header includes at least one of the existence or non-existence of encryption of the content information and the encryption system of the: content information (col.3 lines 23-25; col.4 lines 44-46; col.5 line 65 thru col.6 line 17).

Regarding Claim 3, Komuro et al teach the apparatus according to claim 1, wherein the encryption attribute header includes a copy attribute field having a plurality of bits with regard to the number of copying of the content information (col.6 lines 1-34).

Regarding Claim 5, Komuro et al teach the apparatus according to claim 1, wherein the unit (b) sets the encoding information, which indicates the encoding system for the content information into the expansion transport header or into the payload header (col.4 lines 44-46).

Regarding Claim 6, Komuro et al teach the apparatus according to claim 1, wherein the unit (c) further codes into the basic transport header at least information indicating that there is a possibility that the content information is encrypted, and wherein the unit (b) codes into the expansion header at least information as to whether or not the content information to be transferred is encrypted (col.4 lines 44-46; col.6 lines 1-34; col.6 line46 thru col.7 line 27).

Regarding Claim 7, Komuro et al teach the apparatus according to claim 1, wherein the unit (b) codes into the expansion header information as to whether or not the content information to be transferred is encrypted (col.4 lines 44-46; col.6 lines 1-34; col.6 line46 thru col.7 line 27).

Regarding Claim 8, Komuro et al teach the apparatus according to claim 1, further comprising:

(e) a unit for generating a content attribute header that includes content attribute information with regard to content information, and for setting this content attribute header into the expansion transport header or into the payload header (col.6 line46 thru col.7 line 27).

Regarding Claim 9, Komuro et al teach the apparatus according to claim 8, wherein the content attribute header is not encrypted (col.7 lines 7-9).

Regarding Claim 10, Komuro et al teach the apparatus according to claim 1, wherein the unit (a) generates the encryption key based on an identifier that uniquely identifies a storage medium sent from the other end apparatus in a communication col.12 line 57 thru col.15 line 15).

Regarding Claim 11, Komuro et al teach a content information receiving apparatus authenticated by an authentication process including at least one procedure of an authentication procedure and a key exchange procedure and which receives encrypted content information via a network in accordance with a prescribed transport protocol, comprising:

(aa) a unit for receiving from a sending apparatus a packet containing a basic transport header, an encryption attribute header including attribute information with regard to the encryption of the content information, and encrypted content information (col.8 lines 13-19);

(bb) a unit for referring to the basic transport header or encryption attribute header and judging whether or not the content information is encrypted or whether there is a possibility that the content information is encrypted (col.8 lines 13-19); and

(cc) a unit that, when a judgment is made by the unit (bb) that the content information is encrypted, decrypts the encrypted content information (col.8 lines 23-28), based on the attribute information with regard to encryption included in the encryption attribute header (Figs 4, 5A, 5B; col.7 line 30 thru col.10 line 58).

Regarding Claim 12, Komuro et al teach the apparatus according to claim 11, wherein the unit (bb), when there is a possibility that the content information is encrypted, refers to the encryption attribute header and judges whether or not the content information is encrypted (col.8 lines 15-19).

Regarding Claim 13. Komuro et al teach the apparatus according to claim 11, wherein the unit (bb) refers to the basic transport header or, to the encryption attribute header to make a judgment as to the encoding system of the content information (col.8 lines 15-19).

Regarding Claim 15, Komuro et al teach A method of distributing encrypted content information, via a network in accordance with a prescribed transport protocol, to other end apparatus in a communication authenticated by an authentication process including at least one procedure of an authentication procedure and a key exchange procedure, comprising the steps of:

(a) encrypting content information encoded by a prescribed encoding system (col.7 lines 50-53);

(b) adding an encryption attribute header including attribute information with regard to the encryption of the content information to the encrypted content information (col.7 lines 53-65);

(c) adding a content attribute header indicating attributes of the content information to content information to which the encryption attribute header has been added (col.7 lines 53-65);

(d) performing transport protocol processing required to transfer the content information, and adding a basic transport header to content information to which the content attribute header has been added (col.7 lines 53-65); and

(e) sending a packet including the basic transport header, the encryption attribute header, the content attribute header, and the encrypted content information to the other end authenticated apparatus (col.7 lines 56-58), wherein the encryption attribute header is set into either an expansion transport header within a packet

header of the packet, or into a payload header within an encrypted payload of the packet (Figs 4, 5A, 5B; col.7 line 30 thru col.10 line 58).

Regarding Claim 16, Komuro et al teach a method of distributing encrypted content information, via a network in accordance with a prescribed transport protocol, to other end apparatus in a communication authenticated by an authentication process including at least one procedure of an authentication procedure and a key exchange procedure, comprising the steps of:

(a')adding a content attribute header indicating attributes of the content information to the content information to be transferred;

(b') encrypting content information that are encoded by a prescribed encoding system and to which the content attribute header has been added;

(c') adding to the encrypted content information an encryption attribute header including attribution information with regard to the encryption of the content information;

(d') performing transport: protocol processing required to transfer the content information, and adding a basic transport header to content information to which the encryption attribute header has been added; and

(e') sending a packet including the basic transport header, the encryption attribute header, the content attribute header, and the encrypted content information to the other end authenticated apparatus, wherein the encryption attribute header is set into either an expansion transport header within a packet header of the packet, or into a payload header within a payload to be encrypted of the packet (Figs 4, 5A, 5B; col.7 line 30 thru col.10 line 58).

Regarding Claim 17, Komuro et al teach A method of receiving encrypted content-information, via a network in accordance with a prescribed transport protocol, by an authentication process including at least one procedure of an authentication procedure and a key exchange procedure, comprising the steps of

(aa) receiving a packet including a basic transport header, an encryption attribute header including encryption attribute information with regard to the encryption of the content information and encrypted content information;

(bb) referring to the basic transport header and judging whether or not the content information is encrypted or whether or not there is a possibility that the content information is encrypted;

(cc) referring to the encryption attribute header and extracting encryption attribute information with regard to encryption of the content information;

(dd) referring to an expansion transport header within a packet header of the packet and extracting content attribute information with regard to the; content information; and

(ee) in the case in which a judgment is made at (bb) that the content information is encrypted., decrypting the encrypted content information, based on the extracted encryption attribute information (Figs 4, 5A, 5B; col.7 line 30 thru col.10 line 58).

Regarding Claim 18, Komuro et al teach a method of receiving encrypted content information, via a network in accordance with a prescribed transport protocol, by an authentication process including at least one procedure of an authentication procedure and a key exchange procedure, comprising the steps of:

(aa')receiving a packet including a basic transport header, an encryption attribute header including encryption attribute information with regard to the encryption of the content information and encrypted content information;

(bb') referring to the basic transport header and judging whether or not the content information is encrypted or whether or not there is a possibility that the content information isencrypted;

(cc') in the case in which a judgment is made at (bb') that the content information is encrypted, referring to the encryption attribute header and extracting encryption attribute information with regard to the encryption of the content information;

(dd') in the case in which a judgment is made at (bb') that the content information is encrypted, decrypting the encrypted content information based on the extracted encryption attribute information; and

(ee') referring to an expansion transport header within a packet header of the packet and extracting content attribute information with regard to the content information (Figs 4, 5A, 5B; col.7 line 30 thru col.10 line 58).

Regarding Claim 19, Komuro et al teach A computer-readable recording medium for recording a program to be executed by a computer, the program performing distribution of encrypted content information, via a network in accordance with a prescribed transport protocol, to other end apparatus in a communication authenticated by an authentication process including at least one procedure of an authentication procedure and a key exchange procedure, the program comprising:

(a) a module for generating an encryption attribute header including attribute information with regard to encryption of the content information;

(b) a module for performing transport protocol processing required to transfer the content information and for generating a basic transport header to be added to the content information to which the encryption attribute header has been added; and

(c) a module for sending a packet including the basic transport header, the encryption attribute header, and the encrypted content information to the other end authenticated apparatus, wherein the encryption attribute header is set either into an

expansion transport header within a packet header of the packet or into a payload header within a payload to be encrypted of the packet (Figs 4, 5A, 5B; col.7 line 30 thru col.10 line 58).

Regarding Claim 20, Komuro et al teach a computer-readable recording medium for recording a program to be executed by a computer, the program performing receiving of encrypted content information, via a network in accordance with a prescribed transport protocol, by an authentication process including at least one procedure of an authentication procedure and a key exchange procedure, the program comprising:

(aa) a module for receiving from a sending apparatus a packet including a basic transport header, an encryption attribute header including attribute information with regard to encryption of the content information, and encrypted content information;

(bb) a module for referring to the basic transport header or the encryption attribute header and judging whether or not the content information is encrypted or whether there is a possibility that the content information is encrypted; and

(cc) a module for decrypting the encrypted content information based on attribute: information with regard to encryption included in the encryption attribute header, in the case in which a judgment is made by module (bb) that the content information is encrypted (Figs 4, 5A, 5B; col.7 line 30 thru col.10 line 58).

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claim 4 rejected under 35 U.S.C. 103(a) as being unpatentable over Komuro et al as applied to claims 1 and 11 respectively above, and further in view of Osakabe et al.

Regarding Claim 4, Komuro et al teach the apparatus according to claim 1, but do not teach that the encryption attribute header includes a counter field indicating a change in an encryption key. Osakabe et al teach that the encryption attribute header includes a counter field indicating a change in an encryption key (col.1 lines 56-60; col.3 lines 12-21; col.5 line 63 thru col.6 line 5). It would have been obvious to one of ordinary skill in the art to combine Komuro et al's system for transferring information with Osakabe et al's teaching of using an attribute header that includes a counter field indicating a change in encryption key in order to achieve a higher level of security (Osakabe col.6 lines 3-5).

Claim 14 rejected under 35 U.S.C. 103(a) as being unpatentable over Komuro et al as applied to claim 11 above, and further in view of Markandey et al.

Regarding Claim 14, Komuro et al teach the apparatus according to claim 11, but do not teach a unit for referring to a received basic transport header and, when a prescribed delay time has elapsed or a prescribed number of packets have been discarded, requesting that the sending apparatus send a prescribed encryption parameter. Markandey teach of a unit for referring to a received basic transport header and, when a prescribed delay time has elapsed or a prescribed number of packets have been discarded, requesting that the sending apparatus send a prescribed encryption parameter (col.6 lines 17-45). It would have been obvious of one of ordinary skill in the art to combine Komuro et al's system for transferring information with Markandey et al's teaching of a unit for referring to a received basic transport header and, when a prescribed delay time has elapsed or a prescribed number of packets have been discarded, requesting that the sending apparatus send a prescribed encryption parameter in order to maintain synchronization and to run the verification process (Markandey col.6 lines 44-45).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Tremayne M. Norris whose telephone number is (703) 305-8045. The examiner can normally be reached on M-F 7:30AM-5:00PM alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703) 305-4789. The fax phone number for the organization where this application or proceeding is assigned is (703) 872-9306.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Tremayne Norris

December 23, 2003

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100